Abstract of the Disclosure

A transaction system for use with passive data storage media, such as optical memory cards, uses secure protocols involving digital certificates for communication between a read/write drive and the medium and also for communication between the drive and a host computer. The drive is physically secured with tamper resistant features and stores cryptographic keys and firmware for executing the secure protocols. All messages (data or commands) passed between the drive and the passive medium or host computer not only are encrypted but also include at least one digital certificate for authenticating the message. Typically, asymmetric (public-private key) encryption is used and keys may be derived from an authorized user's password, personal identification number, or biometric data. The drive includes sensors to detect any attempted intrusions and a control unit that will destroy the critical information (keys and protocol code) in response to a detected intrusion. The keys and protocols stored in a drive can themselves be changed through appropriate use of a secure protocol involving digital certificates.